Method and Apparatus for Secure Transmission of Data and Applications

Abstract

Authenticated transmissions are usually time-consuming and often provide delayed error recognition and correction. This is a problem particularly with hand-held computing devices like personal digital assistants (PDAs), smart phones or smartcards, since these usually possess limited memory, processing power and communications bandwidth. Because of these limitations and generally low transfer rates between the device and a provider or central computer base, such transmissions are time-consuming and delay applications. The late detection of unavoidable transmission errors is especially cumbersome. By applying an optimally taylored authentication scheme to a block-wise transmission and in particular by applying a tree structure for the authentication process during such transfers, the present invention minimes the unavoidable delays and thus provides a solution for these problems.